REMARKS/ARGUMENTS

Upon entry of this amendment, claim 1 has been amended and claim 3 has been added. Claims 1-3 remain pending.

Claims 1 and 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Austin (U.S. Pat. No. 4,935,962) in view of Fischer (U.S. Pat. No. 4, 868,877). For the reasons set forth below, Applicant respectfully requests that the rejections be withdrawn.

With respect to claim 1, it has been amended to clarify that the newly generated certificate is for the public key and that the public key is smaller in size than a certificate-signing key contained in the device. The Austin system clearly does not disclose or suggest at least some of the features recited in amended claim 1. For example, Austin does not mention a device being able to generate a certificate for a public key, where the public key is smaller in size than a certificate-signing key stored in the device. As discussed, in Cols. 9 and 10, Austin provides a formula for a new type of signature over a message. The formula, $Y = S_{ID} * \pi_{vi} S_i \text{ (Mod N)}$, is more specifically identified in Col. 9, line 64, where Vi are bit values derived from a general message and S_{ID} is a value signed by a third party such as a certificate authority. As a result, the signature of the device in its computation also includes a signature of the certificate authority.

Furthermore, Austin, in Col. 10, lines 49-51, merely states that "the card could itself produce an authentication certificate for the data emanating from it ... ." There is no mention or suggestion of a newly generated certificate for a public key that is delivered to the device, where the public key is smaller in size than a certificate-signing key stored in the device.

Hence, for at least the foregoing reasons, the amended claim 1 is allowable over the cited art.

With respect to claim 2, this claim depends from allowable claim 1 and thus derives patentability therefrom.

With respect to claim 3, it is believed that this new claim is supported by the specification and does not introduce any new matter. Claim 3 depends from allowable claim 1 and derives patentability therefrom. Notwithstanding the foregoing, claim 3 by itself is also

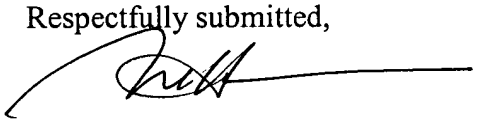
allowable over the cited art. Austin does not mention or suggest having a newly generated certificate that can be used in connection with a smaller public/private key pair.

CONCLUSION

In view of the foregoing, Applicant believes all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,



Horace H. Ng
Reg. No. 39,315

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
Attachments
HHN:hhn
60071621 v1